G-IDS: Generative Adversarial Networks Assisted Intrusion Detection System

Year: 2020 | Citations: 119 | Authors: Md Hasan Shahriar, Nur Imtiazul Haque, M. Rahman

---

Abstract

The boundaries of cyber-physical systems (CPS) and the Internet of Things (IoT) are converging together day by day to introduce a common platform on hybrid systems. Moreover, the combination of artificial intelligence (AI) with CPS creates a new dimension of technological advancement. All these connectivity and dependability are creating massive space for the attackers to launch cyber attacks. To defend against these attacks, intrusion detection system (IDS) has been widely used. However, emerging CPS fields suffer from imbalanced and missing sample data, which makes the training of IDS difficult. In this paper, we propose a generative adversarial network (GAN) based intrusion detection system (G-IDS), where GAN generates synthetic samples, and IDS gets trained on them along with the original ones. G-IDS also fixes the difficulties of imbalanced or missing data problems. We model a network security dataset for an emerging CPS using NSL KDD-99 dataset and evaluate our proposed model's performance using different metrics. We find that our proposed G-IDS model performs much better in attack detection and model stabilization during the training process than a standalone IDS.